PRIVACY IMPACT ASSESSMENT

INTEGRATED BIOMETRIC SYSTEM

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Integrated Biometric System

(b) Bureau: Consular Affairs (CA)

(c) System acronym: IBS

(d) iMatrix Asset ID Number: 877

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization – consolidation of paperwork for legacy systems

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The estimated authorization to operate (ATO) date for IBS is Summer 2018.

(c) Describe the purpose of the system:
The Integrated Biometric System (IBS) supports the Bureau of Consular Affairs mission requirements for issuing visas to foreign nationals and passports to U.S. citizens. The IBS system is an enterprise-level, facial-recognition matching program.

The computerized Face Recognition (FR) has the potential to recognize several photos of the same person in databases that is exponentially larger than those which a human could review. Additionally, automated FR can detect mathematical similarities that could be easily disguised from a subjective human viewer. The use of face recognition technology is used to facilitate anti-fraud goals of the U.S. Department of State's existing travel document issuance processes. IBS provides the Department of State the ability to add, delete, and search millions of photographic images for duplicates prior to the issuance of travel documents.

The IBS FR system provides the Department's consular posts and passport agencies around the world additional information to use to evaluate visa and passport applications, thereby lessening the possibility of a terrorist or criminal being allowed into the United States or receiving a U.S. passport through fraud. The enterprise IBS system contains databases of visa, passport, watch list gallery and Passport Lookout Tracking System (PLOTS) images.

(d) Describe the PII that the system collects, uses, maintains, or disseminates:

The following PII elements are collected and maintained by IBS:

- Photos
- Gender
- Region of residence or nationality
- Birth dates
- Assigned identification number to each record

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

IBS was developed to support U.S. immigration and nationality law as Authorized by the legal authorities listed below:

- 8 U.S.C. 1101- 1504 (Immigration and Nationality Act of 1952, as amended)
- 22 U.S.C 2651(a) (Organization of Department of State)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218 (Passports)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Subchapter E, Visas
- 22 C.F.R. Subchapter F, Nationality and Passports

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- **SORN Name and Number:** Passport Records – STATE 26 and Visa Records – STATE 39
- **SORN publication date:** Passport Records March 24, 2015; Visa Records June 15, 2018

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- Schedule number Department of State Records Disposition Schedule:

A-13-001-16 Passport Lookout Master
Description: This on-line information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
DispAuthNo: N1-059-04-2, item 16

A-13-001-17 Passport Lookout Index
Description: This on-line information system provides rapid access to names in the Passport Lookout Master.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 27)
DispAuthNo: N1-059-04-2, item 17

A-13-001-18 Name Check System (NC)
Description: Name Check History Master. This series contains a yearly listing of requests by Passport Services and Visa Services personnel to query the Passport and Visa Lookout systems (see schedules for A-13-001-16 and 17). The listing provides statistical data for the Bureau of Consular Affairs.
Disposition: Destroy when active agency use ceases.
DispAuthNo: N1-059-04-2, item 18

A-14-001-20 Visa Lookout Master
Description: This on-line series assists visa officers located at posts throughout the world in determining those individuals to whom a visa should be issued or denied. The system functions similarly to the Passport Lookout System (see items 130016 and 130017) by identifying individuals who have been denied visas.
Disposition: Destroy when active agency use ceases.
DispAuthNo: NC1-059-83-4, item 36

A-14-001-21 Visa Lookout Index

Description: This on-line series provides rapid access to names in the Visa Lookout Master. Searches may be by name, date of birth, or visa office.
Disposition: Destroy when active agency use ceases.
DispAuthNo: NC1-059-83-4, item 37

A-14-001-24 Name Check System (NC)
Description: Name Check History Master. This series contains a yearly listing of requests by Passport and Visa Office personnel to query the Passport and Visa Lookout systems (see items 140020 and 140021). The listing provides statistical data for the Bureau of Consular Affairs.
Disposition: Destroy when active agency use ceases
DispAuthNo: NC1-059-83-04, item 23

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No No SSNs are collected.

- If yes, under what authorization?

(c) How is the information collected?

IBS receives its data directly from the Consular Consolidated Database (CCD) within CA/CST. Information in CCD is extracted from both visa and passport applications and from a direct Terrorist Screening Center (TSC) feed.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

Accuracy is the responsibility of the source that originally collected the data, e.g., the post that submits a photo and its identifiers for comparison. IBS' built-in constraints require completion of all fields. If a record is missing information, the record is stored in a queue and reviewed prior to being added into the system. Additionally, IBS performs quality checks on each image prior to being added into the system.

The IBS FR application can detect mathematical similarities that could be easily disguised from a subjective human viewer. Pattern recognition of photographic elements is coupled with biographical text.

The IBS Facial Recognition (FR) program for visas checks the photos against two galleries:

- The Visa Gallery is comprised of visa applicant photos, including Category One and Two Refusals.
- The Watch List gallery is comprised of photos from the National Counterterrorism Center via the Terrorist Screening Center.

The IBS FR program for passports checks the photos against four galleries:

- The Passport Gallery is comprised of previous passport applicant photos.
- The PLOTS gallery is comprised of potential or known fraudulent passport applicants.
- The watch list gallery is comprised of photos from the National Counterterrorism Center via the Terrorist Screening Center.
- The Visa Gallery is comprised of visa applicant photos, including Category One and Two Refusals.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

IBS data is current and constantly kept up-to-date via enrollment and un-enrollment requests routed to IBS via the Consular Consolidated Database (CCD). The IBS FR system retrieves requests from the CCD. After processing each request, the IBS FR system notifies the CCD that the request has been processed. The FR system performs automated, periodic (multiple times per hour) validations to ensure data integrity.

(g) Does the system use information from commercial sources? Is the information publicly available?

No. The system does not use commercial information, and the information is not publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

IBS does not directly collect personal information from applicants. The identifying information and photos have been submitted by the visa or passport applicant prior to electronic transfer to IBS. The visa application form contains a confidentiality statement indicating that visa records are confidential under INA 222(f) and can only be used for specific purposes including administering and enforcing U.S. immigration laws. All passport application forms contain a Privacy Act disclosure stating that one of the purposes for soliciting the information on the form, including the personally identifiable information (PII) entered into IBS, is to establish the identity of the applicant. Additionally, notice of the use of personal information is provided through the two SORNs mentioned above, State-39 and State-26.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, **how** do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

IBS does not directly collect personal information from applicants; therefore, opportunity and/or right to decline options do not directly apply to this system. IBS is used to perform a Face Recognition check on all visa and passport applicants. The information and photographic images entered into IBS are given voluntarily by the applicant as part of the visa or passport application process. An applicant may refuse to provide the requested information, but doing so may result in the denial of the application.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII collected by IBS is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The PII collected enables the system to search millions of photographic images for duplicates or matches prior to the issuance of travel documents. By performing this function, the Department greatly lessens the threat of issuing passports or visas to known criminal threats and fraudulent actors.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes – The information collected supports the implementation of the State Department's visa and passport programs. The information is used to support visa and passport application submission, processing, and approval/denial decisions.

(c) Does the system analyze the information stored in it?

☒Yes

☐No

If yes:

(1) What types of methods are used to analyze the information?
IBS provides image verification, which is the one-to-one comparison of a known image against a submitted image for assessment and scoring. IBS also provides identification, which is the one-to-many comparison of a captured image against a database of images. The search returns a list of potential matches, typically ranked in score for matching probability. IBS uses analysis of photographic images to determine similarities and determine probability rankings.

(2) Does the analysis result in new information?
Reports on the applicant and possible matching images from the database are produced for analysis which can produce new information. Statistical reports summarize metrics based on the number of record enrollments, searches, deletions, and volumes.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☒Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
The only internal organization that has access to IBS data is the Bureau of Consular Affairs (CA). IBS does not share any information directly with external agencies. FR matching results are shared with external agencies via the Consular Consolidated Database (CCD), which has Integrated Biometric System (IBS) extensive user authentication, role-based users and data

encryption in place. U.S. Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) of the Department of Homeland Security and the National Counterterrorism Center (NCTC) have access to the FR data via the CCD for the purpose of enforcement of the Immigration and Nationality Act (INA) and for counterterrorism purposes.

The CCD is the single interface for all incoming requests processed by IBS, as well as all outgoing results. IBS interfaces with the CCD via secure transmission methods permitted by internal Department of State policy for the handling and transmission of Sensitive But Unclassified (SBU) information.

Access to the IBS application is strictly limited to authorized users to perform visa and passport functions and system administrators. Audit trails track and monitor usage and access. Regularly administered security and privacy training informs authorized personnel of proper handling procedures.

(b) What information will be shared?
The data processed in IBS includes photos, gender, region, and birth dates, as well as an assigned identification number for each record.

(c) What is the purpose for sharing the information?
CA is responsible for issuing visas to foreign nationals and passports to U.S. citizens and non-U.S. citizen nationals. Inherent in these responsibilities is the obligation to verify applicant identities, to prevent the issuance of travel documents to those who pose national security threats, and to prevent the issuance of travel documents to applicants using fraudulent aliases. IBS results are used as a data source for this assessment at posts abroad and domestic passport agencies. The IBS FR system provides information to the Department's consular posts and passport agencies, and external agencies for use in evaluating visa and passport applications, thereby lessening the possibilityof a terrorist or criminal being allowed into the United States or receiving a U.S. passport through fraud.

(d) The information to be shared is transmitted or disclosed by what methods?

The information is shared by secured internal connections within the Consular Affairs Consular Consolidated Database (CCD) system. Both of these systems reside on the Department's secure intranet network, OpenNet. Information shared externally is exchanged through the CCD and utilizes connection security and service agreements.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal recipients within the Department of State are required to comply with U.S. government requirements for the protection and use of PII. These safeguarding requirements include, but are not limited to, security training and following internal Department policy for the handling and transmission of "Sensitive But Unclassified" information. In addition, all Department users are required to attend annual privacy and security awareness training to reinforce safe handling practices. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

Information is shared though an interconnection with the Consular Consolidated Database (CCD) by secure transmission methods permitted by internal Department policy for the handling and transmission of Sensitive But Unclassified (SBU) information.

Supervisors along with information system security officers determine the access level depending on job function and level of clearance. Access to the IBS application is strictly limited to management and system administrators. Contractor system administrators are the only individuals who have direct access to the system. Audit trails track and monitor usage and access of all users.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:
Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft of information to non-authorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

2) Strict role based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level

3) System authorization and accreditation process along with continuous monitoring via Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

4) All communications shared with external agencies are via the CCD and encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
IBS receives its data from the Consular Consolidated Database (CCD) within CA/CST. Information in CCD is extracted from both visa and passport applications and from a direct Terrorist Screening Center (TSC) feed. The individual would need to follow processes outlined by the source system CCD to request access to their information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Individuals must follow processes of the source system CCD to request correction of information. Notice to change personal information is provided at the site where applicants apply for specific services.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

The IBS does not collect PII from individuals and only pulls PII information from the CCD database, which resides outside the IBS system boundary. Notification is the responsibility of the system that collects the information directly from the individual.

8. Security Controls

(a) How is the information in the system secured?

The system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The level of access granted to IBS restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited.

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with State Department Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System (OS) Level auditing is set in accordance with the State Department Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training and pass the Privacy Act PA-459 course, Protecting Personally Identifiable Information. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. The security measures are in place to minimize that risk, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?
Access to the IBS application is strictly limited to authorized users (visa and passport personnel) and systems administrators.

(b) How is access to data in the system determined?

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?
☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than the administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges, which are restrictive rights/privileges or accesses needed by users for the performance of specified tasks, are implemented. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN), and activities while logged in can be traced to the person that performed the activity. Users are aware of this by reading and clicking ‘I agree’ to the logon banner.